
3Com OfficeConnect VPN Firewall Software Version 2.02 Release Notes

Product Number: 3CR870-95

This document provides the following information:

1. Legal Rights
2. Fixes in this release
3. Recommendations when using this release
4. Known problems with this release
5. Upgrading Your Software
6. 3Com's World Wide Web site

Please use these notes in conjunction with the following document:

"OfficeConnect VPN Firewall User Guide"
Part number: DUA08709-5AAA04

1. Legal Rights

IMPORTANT: READ THIS BEFORE INSTALLING OR USING THIS SOFTWARE

You should carefully read the terms and conditions of the Software License Agreement. This text is supplied with your Firewall, and also contained in a file called license.txt on the Firewall's CD-ROM.
Your legal rights are defined therein.

USE OF THIS SOFTWARE INDICATES THAT YOU ACCEPT SUCH TERMS AND CONDITIONS.
IF YOU DO NOT AGREE WITH SUCH TERMS AND CONDITIONS, DO NOT USE THIS SOFTWARE.

2. Fixes between 2.01 and 2.02 releases

- The total number of sessions has been limited with 1440. Once the session number reaches 1024, the sessions start getting cleaned aggressively. The aggressive timeout is 60 seconds i.e all sessions older than 60 seconds start getting cleaned. Once the number of sessions drops below 1024 the session cleaning is stopped.
- The session cleaning is handled by a timer thread ("tALCwTimer"). It was running every 500 ms to clean sessions. It is now made to run every 50 ms so that when the sessions are in huge number the timer thread cleans them as quickly as it can.
- The issue with PC Privilege that the DNS traffic from the local out was getting blocked on firewall has been fixed.
- One crash when box is trying to get connected as a PPPoE client has been identified and fixed.
- One crash on user mode when packets which has not been belonging to any of the interfaces is entering into DNS loopback, is fixed.

- A crash on ALIKE daemon task is fixed by merging the two tasks "ALIKE_d" and "ALIKEMONITOR since the crash is identified as these are trying to access/free common objects in the VPN.
- The maximum URL size is increased to 2048 as it is recognised to cause problem in content filtering.
- The PPPoE issue with some servers is fixed, as the box will remove the existing AP protocol objects whenever LCP re-establishes, to make it compatible with such server behaviour. Updates for handling LCP/AP connection abort is added.
- Updates for VPN hangs issue when simultaneous negotiation happens is included.
- The issue of VPN with 1-2-1 NAT is not working is solved by adding the static IPs with mask 255.255.255.255 for each 1-2-1 NAT alias interfaces.
- Updates to resolve VPN issue with INVALID_MAJOR_VERSION error when re-negotiating Phase 2 is added. The root cause is that phase 2 negotiation is three-message exchange, there is a chance that because the last phase 2 message is processed by IKE, IPsec packet has already arrived. In NAT traversal scenario, the IPsec packet is encapsulate in IKE NAT-T UDP, thus, will reach IKE daemon. The update prevents IKE from processing IPsec NAT-T packet.
- PPTP would fail with no such user message just after the boot time since the VPN requires 5 minutes delay to complete its configuration. Now the VPN will complete its configuration when the box rebooted.
- Fixed an issue with Safenet client that safenet client is not renegotiating phase1 after the SA life timeout. VPN Firewall is modified to make it compatible with safenet client's behaviour.

3. Recommendations when using this release

4. Known problems with this release

- The VPN is updated to start without any delay. Though the other components

like content filtering, NTP etc will take 5 minutes delay to start in action.

5. Upgrading Your Software

Although the upgrade process has been designed to preserve your configuration settings, 3Com recommends that you make a backup of the configuration before upgrading, in case the upgrade process fails (for example, the connection between the computer and the Firewall may be lost while the new software is being copied to the Firewall).

3Com also recommends that VPN users are disconnected and the Firewall is rebooted before starting the upgrade process.

To upgrade the OfficeConnect VPN Firewall:

1. Ensure that the Firewall is powered and a link is established with the host PC.
 2. Ensure that the latest version of the Firewall firmware is located on the host PC. The latest version of the OfficeConnect VPN Firewall software can be obtained from the following Web site:
<http://support.3com.com>
 3. Launch a web browser to the IP address of the Firewall and log in.
 4. Select 'System Tools' from the menu bar on the left hand side of the screen.
 5. Select the 'Upgrade' tab.
 6. Browse to the location of the Firewall firmware, select the file and press the Apply button. You may need to change the file type in the dialog box to *.* to see the upgrade file.
 7. Wait for the upgrade process to complete. This may take several minutes and is complete when the Alert LED has stopped flashing and stays off.
-

6. 3Com's World Wide Web site

Access the latest networking information on the 3Com Corporation World Wide Web site by entering the following URL into your Web browser:

<http://www.3com.com/>

You will find software upgrades, troubleshooting guides and other support information at the 3Com support site:

<http://support.3Com.com/>

For any additional information related to known issues on 3Com products please see also:

<http://knowledgebase.3com.com>

7. Documentation Errors and Omissions

None

(R) means registered trademark.

3Com and OfficeConnect are registered trademarks of 3Com Corporation.

Other trademarks are the property of their respective owners.

Document Number: DNA08709-5AAA04v2.01

Issued: October 2005

Copyright (c) 2005 3Com Corporation. All Rights Reserved.